

# The Silent Risk We are Living With INSIDER THREAT

Pan Kamal, CISA  
AlertEnterprise, Inc.

ICSJWG 2010 Spring Conference

# This is How Organizations Manage Insider Threat Today...



It's a silent risk they're living with...

# Outline

Headlines you don't want to be in

Insider Threat Examples

Insider Threat Characteristics – CERT SEI Carnegie Mellon

Real World Incidents don't discriminate

Challenges, Silos, Blended Threats

Threat Scenarios :

- Terminated Employee access to SCADA
- Smart Meter Disconnect
- Sabotage Attempt

Recommendations

# Headlines you don't want to be in...

## Enterprise Access Security News

TODAY'S EDITION

### "Dummy" Employee Scandal at Satyam

Aliquam erat volutpat. Sed quis velit. Nulla facilisi. Nulla libero. Vivamus pharetra posuere sapien. Nam consectetur. Sed aliquam, nunc eget euismod ullamcorper, lectus nunc ullamcorper orci, fermentum bibendum enim nibh eget ipsum.

Donec portitor ligula eu dolor. Maecenas vitae nulla consequat libero curva venenatis. Nam magna enim, accumsan eu, blandit sed, blandit a, eros. Quisque facilisis erat a dui. Nam malesuada cenase dolor. Cras gravida, diam si amet rhoncus ornare, erat elit consectetur erat, id egestas pede nibh eget odio.

Proin tincidunt, velit vel porta elementum, magna diam.

Suspendisse sagittis ante a urna. Morbi a est quis orci consequat rutrum. Nullam egestas frugiat felis. Integer adipiscing semper ligula. Nunc molestie, nunc sit amet curvas convallis, sapien lectus pretium metus, vitae peritum enim wisi id lectus. Donec vestibulum.

Etiam vel nibh. Nulla facilisi. Mauris pharetra. Donec augue. Fusce ultrices, neque id dignissim ultrices, tellus mauris dicitur elit, vel lacinia enim metus eu nunc. Proin at eros non eros adipiscing mollis.

Donec semper turpis sed diam. Sed consequat ligula nec tortor. Integer eget sem. Ut vitae enim eu est vehicula gravida. Morbi ipsum ipsum, porta nec.

### Angry Ex-engineer Plants Malicious Code in Fannie Mae network

conmodo, ipsum sed pharetra gravida, orci magna rhoncus neque, id pulvinar odio lorem non turpis. Nullam sit amet enim. Suspendisse id velit vitae ligula volutpat condimentum.

Aliquam erat volutpat. Sed quis velit. Nulla facilisi. Nulla libero. Vivamus pharetra posuere sapien. Nam consectetur. Sed aliquam, nunc eget euismod

ullamcorper bibendum enim nibh eget ipsum. Donec portitor ligula eu dolor. Maecenas vitae nulla consequat libero curva venenatis. Nam magna enim, accumsan eu, blandit sed, blandit a, eros. Quisque facilisis erat a dui. Nam malesuada cenase dolor. Cras gravida, diam si amet rhoncus ornare, erat elit consectetur erat, id egestas pede nibh eget odio.

convallis, sapien lectus, vitae pretium lectus. Donec vestibulum, vitae peritum enim wisi id lectus. Donec vestibulum. Etiam h. Nulla facilisi. Mauris a. Donec augue. Fusce neque id dignissim

Proin at eros non eros adipiscing mollis. I turpis sed diam. Sed

### Former Auditor at Cal Water Executes Fraudulent Wire Transfers after Resigning

Locum ipsum dolor sit amet, consectetur adipiscing elit. Morbi conmodo, ipsum sed pharetra gravida, orci magna rhoncus

Integer adipiscing semper ligula. Nunc molestie, nunc sit amet curvas convallis, sapien lectus pretium metus, vitae peritum enim wisi id lectus. Donec vestibulum. Etiam h. Nulla facilisi. Mauris a. Donec augue. Fusce neque id dignissim

Proin at eros non eros adipiscing mollis. Donec semper turpis sed diam. Sed consequat ligula nec tortor. Integer eget sem. Ut vitae enim eu est vehicula gravida. Morbi ipsum ipsum, porta nec, tempus id, auctor vitae, purus. Pellentesque neque.

### Countrywide Analyst Steals Customer SSNs

Integer facilisis erat a dui. Nam malesuada ornare dolor. Cras

gravida, diam sit amet rhoncus ornare, erat elit consectetur erat, egestas pede nibh eget odio.

Proin tincidunt, velit vel porta elementum, magna diam molestie nunc, nunc aliquet magna pede ornare. Aliquam laculis. Fusce et urn et nulla tristique facilisis.

Donec eget sem sit amet ligula convallis.

### Reset Passwords at City of San Francisco Locks Network

consectetur adipiscing elit. Morbi conmodo, ipsum sed pharetra gravida, orci magna rhoncus neque, id pulvinar odio lorem non turpis. Nullam sit amet enim. Suspendisse id velit vitae ligula volutpat condimentum.

Aliquam erat volutpat. Sed quis velit. Nulla facilisi. Nulla libero. Vivamus pharetra posuere sapien. Nam consectetur. Sed aliquam, nunc eget euismod.

Nunc molestie, nunc sit amet curvas convallis, sapien lectus pretium metus, vitae peritum enim wisi id lectus. Donec vestibulum. Etiam vel nibh. Nulla facilisi. Mauris pharetra. Donec augue. Fusce ultrices, neque id dignissim ultrices, tellus mauris dicitur elit, vel lacinia enim metus eu nunc. Proin at eros non eros adipiscing mollis.

Donec semper turpis sed diam. Proin at eros non eros adipiscing mollis. Donec semper turpis sed diam. Sed consequat.

### Drug Diversion Scandal at Cardinal Health

Nulla facilisi. Mauris pharetra. Donec augue. Fusce ultrices, neque id dignissim ultrices, tellus mauris dicitur elit, vel lacinia enim metus eu nunc. Proin at eros non eros adipiscing mollis.

Donec semper turpis sed diam. Sed consequat ligula nec tortor.

### Disgruntled Ex-contractor Brings Down Network for 2 Weeks at Pacific Energy

Proin at eros non eros adipiscing mollis. Donec semper turpis sed diam. Sed consequat ligula nec tortor. Integer eget sem. Ut vitae enim eu est vehicula gravida. Morbi ipsum ipsum, porta nec, tempus id, auctor vitae, purus. Pellentesque neque.

Nulla lacus erat vitae libero. Integer nec enim. Phasellus aliquam enim et tortor. Quisque

Prosect ultrices facilisis nisl. Vivamus lacus elit sit amet mi. Phasellus pellentesque, erat eget elementum volutpat, dolor nisl porta neque, vitae sodales ipsum nibh in ligula. Maecenas mattis pulvinar diam. Curabitur sed leo. Nulla facilisi. In vel sem. Morbi id urna in diam dignissim frugiat. Proin molestie tortor eu velit.

# Ghost Employee Fraud

## "Dummy" Employee Scandal at Satyam

Aliquam erat volutpat. Sed quis velit. Nulla facilisi. Nulla libero. Vivamus pharetra posuere sapien. Nam consectetur. Sed aliquam, nunc eget euismod ullamcorper, lectus nunc ullamcorper orci, fermentum bibendum enim nibh eget ipsum.

Donec porttitor ligula eu dolor. Maecenas vitae nulla consoquat libero curvato variatis. Nam magna enim, accumsan eu, blandit sed, blandit a, eros. Quisque facilisis erat a dui. Nam malesuada ornare dolor. Cras gravida, diam sit amet rhoncus ornare, erat elit consoquat erat, id eget pede nibh eget odio. Proin tincidunt, velit vel porta elementum, magna diam.

Suspendisse sagittis ante a urna. Morbi a est quis orci consoquat rutrum. Nullam egetas frugiat felis. Integer adipiscing semper ligula. Nunc molestie, nisl sit amet cursus consoquat, sapien lectus pretium metus, vitae porttitor enim wisi id lectus. Donec vestibulum.

Etiam vel nibh. Nulla facilisi. Mauris pharetra. Donec augue. Fusce ultrices, neque id dignissim ultrices, tellus mauris dui enim elit, vel lacinia enim metus eu nunc. Proin at eros non eros adipiscing mollis.

Donec semper tunc sed diam. Sed consoquat ligula nec tunc. Integer eget sem. Ut vitae enim eu est vehicula gravida. Morbi ipsum ipsum, porta nec.

- Major Outsourcing company recorded payments to 13,000 non-existent employees
- Internal controls and auditors could not detect incident
- Disclosed by whistleblower

- These employees never entered a company facility
- No laptop cell phone etc were issued
- This group never accessed any applications

# Drug Diversion Scandal

- Employees with privileged access were scrapping inventory of high-value pharmaceuticals
- These were sold via online retail sites
- Company forced to pay large settlement to suppliers

•Critical Physical and Logical Access Violations

- No enhanced monitoring for personnel with critical access

## Drug Diversion Scandal at Cardinal Health

*Nulla facilis. Mauris pharetra.  
Donec augue. Praesent ultrices,  
neque id dignissim ultrices, tellus  
mauris dictum elit, vel lacinia  
enim metus eu nunc. Proin at eros  
non eros adipiscing mollis.  
Donec semper turpis sed diam.  
Sed consequat ligula nec tortor.*

# Former Employee Access Un-Revoked



## Former Auditor at Cal Water Executes Fraudulent Wire Transfers after Resigning

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas ornare, ipsum sed pharetra gravida, nisi magna rhoncus magna, id pulvinar odio lorem non nunc. Nullam sit amet enim. Suspendisse id velit vitae ligula volutpat condimentum.

Integer adipiscing semper ligula. Nunc molestie, nisi sit amet cursus ornare, sapien lectus pretium metus, vitae pretium enim wisi id lectus. Donec venenatum. Etiam vul nibb. Nulla facilisi. Maecenas pharetra. Donec augue. Fusce ultrices, neque id dignissim

Proin at eros non eros adipiscing mollis. Donec semper turpis a diam. Sed consequat ligula nunc. Integer eget sem. Ut enim eu est vehicula gravida. Maecenas ipsum ipsum, porta tempor id, nunc vitae, posuere pellentesque neque.

- Former internal auditor's physical access remained active
- Entered VP's office and completed 3 wire transfers totaling \$9Million
- Still remains at large

- No process for timely removal of physical access
- No automated monitoring for off-hours access to treasury applications

# Unauthorized Change Causes Blackout

**Florida Power & Light  
engineer causes  
extensive blackout**

*Mulla laudat. Mauna pharetra.  
Donec augue. Fusce ultrices, tellus  
mauris dictum elit, vel lacinia  
conit metus eu nunc. Proin at cona  
non eros. adipiscing mollis.  
Donec semper turpis sed diam.  
Sed consectetur ligula nec tortor*

- Unauthorized disabling of protective relays by field personnel. Change to control systems configuration undetected.
- Most extensive blackout, 600,000 customers in the southeast left without power
- Company to pay fines in excess of \$100 million

- Control Systems operate in silos
- Unable to detect unauthorized configuration changes
- Unable to respond to incident



# Disgruntled Employee Eliminates Preservatives

- Disgruntled process employee changes settings to eliminate addition of preservatives
- Packaged food ships out causing many to fall ill and severely impacting manufacturers reputation

- No risk analysis with HR records to identify disgruntled employee
- Inability to detect change of configuration or process settings

## Food Processing Plant Faced With Contamination Fines

*Mulla laetitia. Mauris pharetra.  
Donec augue. Praesent ultrices,  
neque id dignissim ultrices, tellus  
mauris duiam elit, vel lacinia  
enim metus eu nunc. Proin at cras  
non eros. Adipiscing mollis.  
Donec semper turpis sed diam.  
Sed consequat ligula nec tortor.*

# Theft of Customer Information

## Countrywide Analyst Steals Customer SSNs

Quisque facilisis erat a dui. Nam malesuada ornare dolor. Cras gravida, diam sit amet rhoncus ornare, erat elit consectetur erat, id agestas pede nibh eget odio. Proin tincidunt, velit vel porta elementum, magna diam molestie sapien, non aliquet massa pede eu diam. Aliquam iaculis. Prae et ipsum et nulla tristique facilisis. Donec eget sem sit amet ligula viverra ornare.

- IT Analysts enters data center after hours
- Accesses confidential customer data, and sells customer SSNs to organized crime ring

- No active monitoring or alerting of after hours physical access
- No correlation with access to confidential information

# Financial Fraud - Unrestricted Access

## Finance Manager Creates Fictitious Vendors

Quisquam facilis erat a dui. Nam  
malesuada ornare dolor. Cras  
gravida, diam sit amet rhoncus  
ornare, vari etit consectetur erat.  
id egestas pede nibh eget odio.  
Proin tincidunt, velit vari porta  
elementum, magna diam molestie  
scipiam, non aliquet massa pede eu  
diam. Aliquam tincidunt. Fusce et  
ignam et nulla tristique facilis.  
Donec eget vari sit amet ligula  
viverra ornare.

- Finance manager has access to accounts payable applications and physical access to check printing room
- Creates fraudulent payments and collects checks from printing room undetected

- No active monitoring of SOD violations across physical and logical applications

# Insider Characteristics

## Majority of Insiders were Former Employees

- At the time of the incident, 59% of the insiders were former employees or contractors
- Reason for Employees Departing:
  - 48% Fired
  - 38% Resigned
  - 7% Laid Off

Source: CERT, Software Engineering Institute, Carnegie Mellon

# Many of the Insiders were “Techies”

## **86% of the Employees were Technical**

- 38% System Administrators
- 21% Programmers
- 14% Engineers
- 14% IT Specialists

## **Non Technical**

- 10% Managerial / Professional / Audit
- 4% Customer Services/ Other services

**No Automated Process to Manage and Monitor Privileged User Access**

Source: CERT, Software Engineering Institute, Carnegie Mellon

# Thirty Percent Of Insiders Had a Criminal Past AND Had Been Arrested

18% Arrests for violent offenses

11% Alcohol or Drug offenses

11% Simple Theft (non-fraud, non-financial)

80% Were noticed by co-workers – acting strangely.

31% of the insiders had a record of disciplinary actions within the organization prior to the incident.

If only someone could have correlated the HR records to access entitlements.

Source: CERT, Software Engineering Institute, Carnegie Mellon

# Detecting Incidents / Identifying Perpetrators

63% of the incidents were detected due to an irregularity

42% detected after system failed

10% detected due to irregularity followed by failure

In 41% of the cases the insider was identified through forensic examination of organizations network, computers, systems. 24% through examination of the insider's home system.

Source: CERT, Software Engineering Institute, Carnegie Mellon

# Many Organizations Faced Financial Impacts from Insider's Activities

- Financial Loss
- Adverse Impact to Business Operations
- Damage to Reputation

58% of the organizations experienced financial impact of \$20,000 all the way up to \$10 Million

Source: CERT, Software Engineering Institute, Carnegie Mellon



# Insider's Goal

51% Sabotage IT Networks / Systems

51% Sabotage Business

49% Sabotage Information / Data

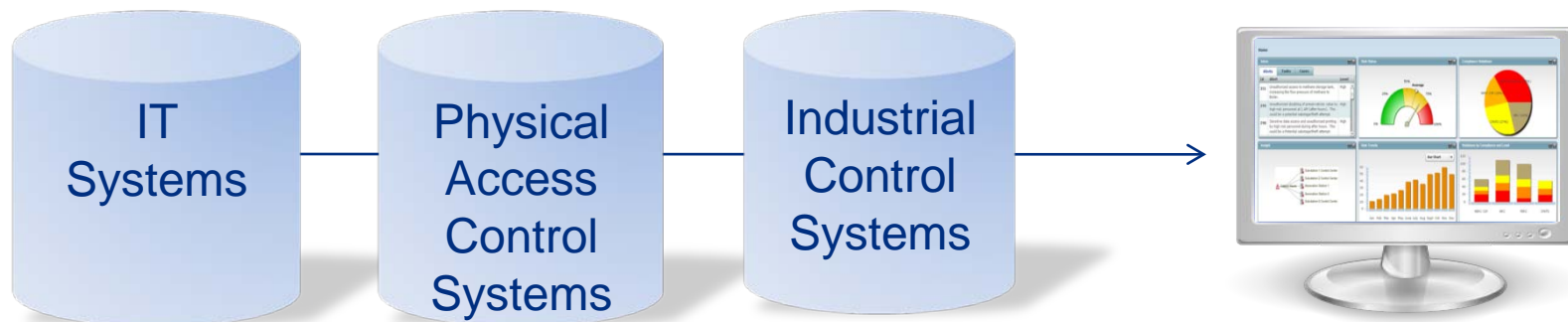
35% Harm specific Individuals

25% Sabotage the organization's reputation

Source: CERT, Software Engineering Institute, Carnegie Mellon

# Real-World Security Incidents Don't Discriminate...

**Real world security incidents don't come neatly packaged as IT incidents and non-IT incidents.**



**Converging IT Security. Physical and Industrial Controls  
Enables a World-Class Response to Real-World  
Incidents**

# Complex Risks and Security Challenges

## Threats

- Physical and Cyber protection of sensitive assets
- Critical Asset Diversion (Dangerous Chemicals, Pathogens, Nuclear material )
- Cyber Attacks - Utilities (Water, Power, Gas), Smart Grids, Transportation
- Terrorism (Chemicals stolen to make explosives)
- Bio Terrorism (Food & Beverage, Consumer Products)
- Fraud (Fake employees/contractors)
- Disgruntled employees/contractors (both current and past)

## Monitoring both Access and Behavior

- Do right people have access to assets (job, certifications, background)
- Any suspicious behavior or activities
- Monitoring Privileged Users and “Access Creep”

## Effective Response, Command and Control

- Situational Awareness, Incident Management, First Responder Card

# Incident Management Challenges

## **Geographically Dispersed assets/locations**

- Guards with guns – expensive and not cost-effective
- Impossible to cover all locations
- Putting guards/employees at unnecessary risk

## **3 ring binders approach – not suitable for modern times**

- We are up against Organized and State Sponsored Crime
- Response has to be instant and appropriate

## **Audit trail of incident management – very important**

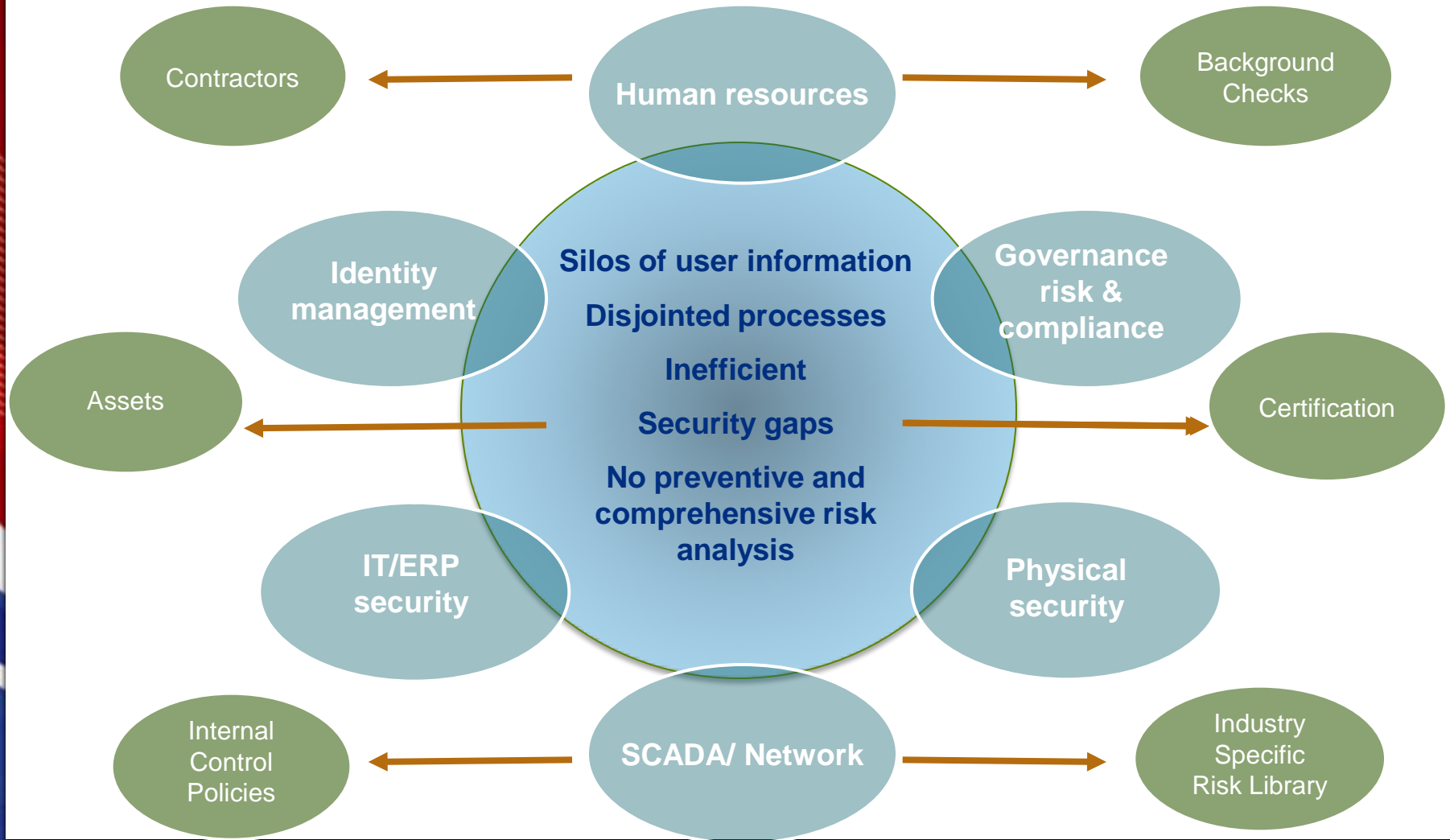
- How incident was handled – to learn from mistakes for future
- Making sure no one took advantage of an emergency
- Monitoring First Responders (with privilege comes accountability)

## **Leveraging investments in technology**

- Non-lethal weapon systems (rubber bullets, sticky foam, non-lethal gas)
- Cameras, sensors, alarms, physical access control systems etc.

# Problem/Challenge: Too Many Silos

*(inefficient, expensive, fraught with risk)*



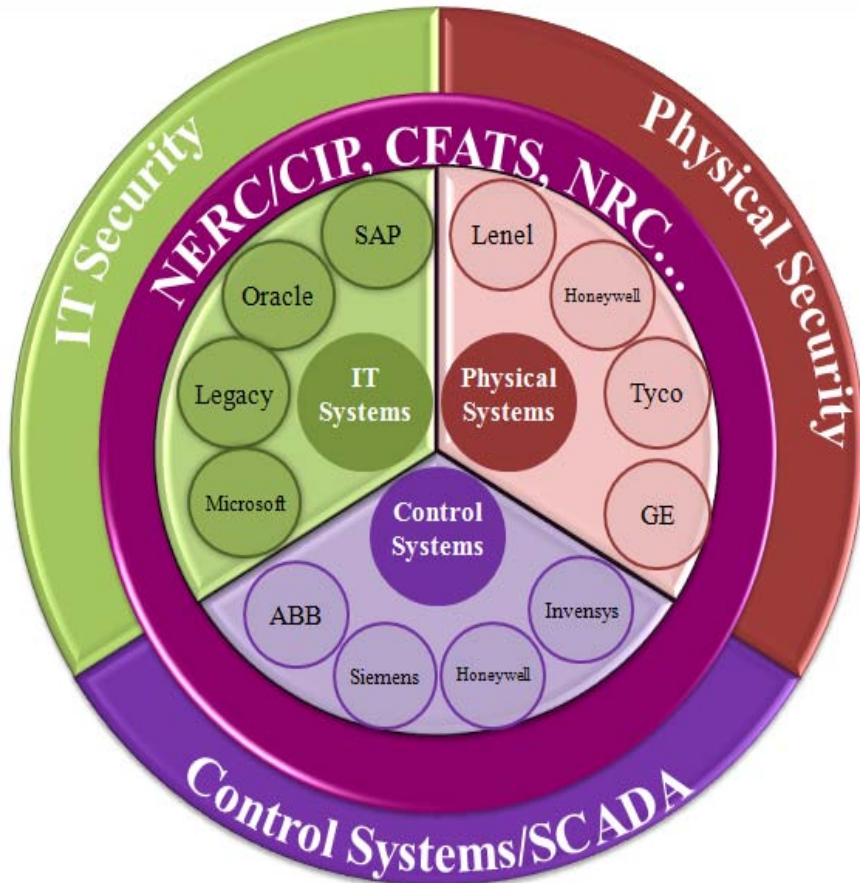
# Streamlining On-boarding/Off-boarding & Close Security Gaps



# Addressing Blended Threats

The Problem:

The Solution:



## Unique capabilities:

- True prevention of threats from theft, fraud, sabotage and terrorism
- Rule based risk analysis across IT, Physical & Industrial Control Systems
- Take Incident management to the next level with built-in programmed remediation
- Built-in intelligence (domain/application context)

# Threat Scenarios

**The following examples are scenarios where detecting blended threats across IT, Physical Access and Control Systems can Detect and Prevent incidents from occurring:**

1. Terminated Employee(s) have access to SCADA assets
2. Disgruntled Employee Attempts Smart Meter Disconnect
3. Utility Employee Enters Remote Substation with Intent to Sabotage Grid



# Threat Scenario #1 - Terminated Employees have Access to SCADA

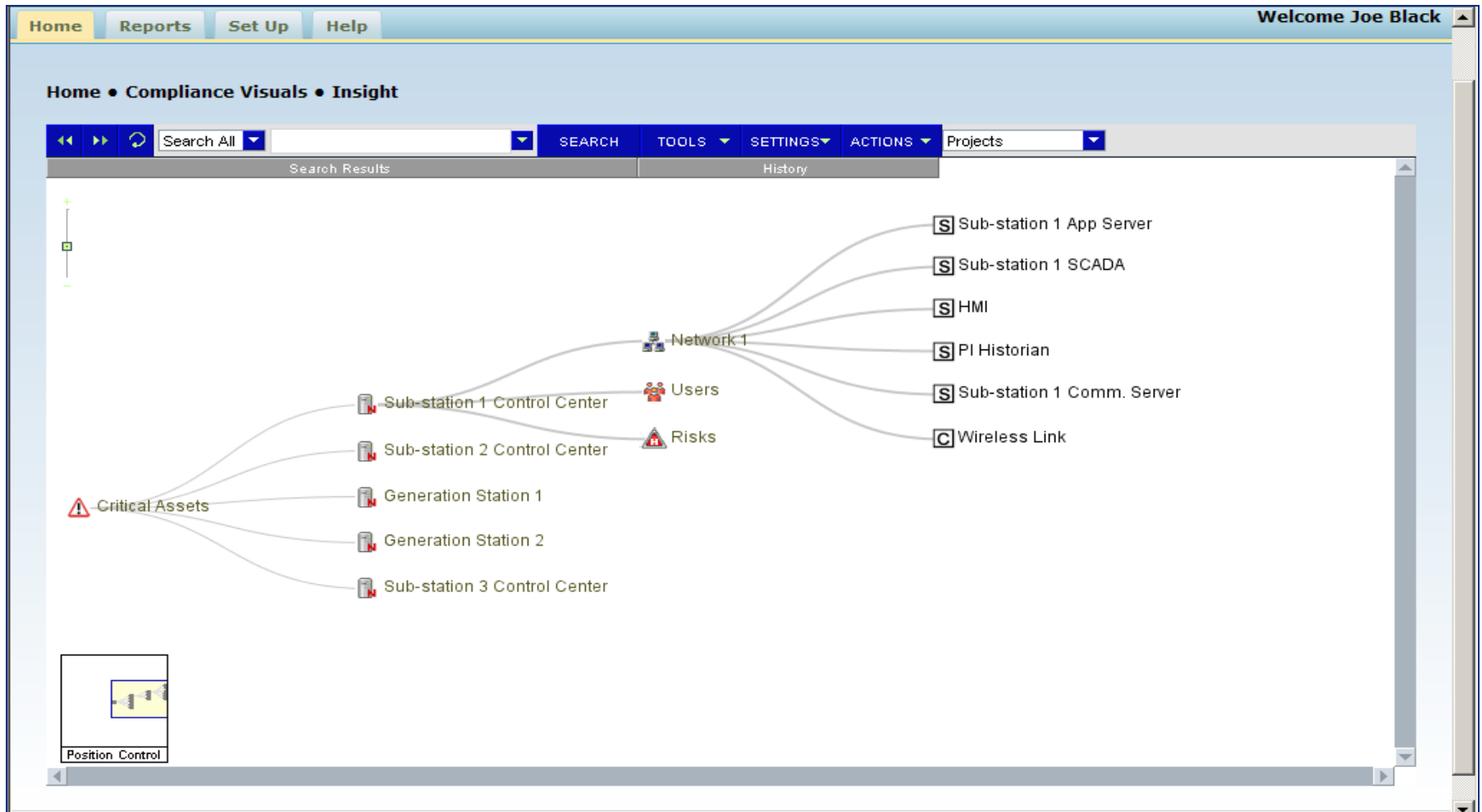
Can you determine risk from this table?

DOCUMENT TITLE: <b>CIP-002-1   Critical Cyber Assets</b>	EFFECTIVE DATE: <b>10-Jan-2008</b>	DOCUMENT NO. <b>BES-01-002</b>
DOCUMENT OWNER: <b>Director, Transmission Services</b>	REVISED DATE: <b>4-Feb-2009</b>	REV.VER. <b>1.1Draft</b>
APPROVED BY: <b>VP Electric Utilities VP Generation</b>	APPROVED DATE:	Page (Format Dependent) <b>Data File</b>

Risk Priority Number =  
BES x Cyber x Level

Reference # or Drafting Code	Owning Entity	Operating Entity	Asset Description	R1.2 Asset Category	Asset Level	BES-01-001 Basis Document Section	Control Station	Communication	Restoration	Level (Drafting)	Protection Scheme	Addressed Assets	R.2 BES Critical	Notes on Criticality of Assets	CIP-002-1 R3 Cyber Asset Identification	R3 Cyber Asset	Notes on Asset Cyber Criticality	"B" Asset Risk Assessment (1=Low to 5=High)	Risk Level	RPN	Security Actions Required			
																					Critical Cyber Asset?	Electronic Security Perimeter?	Secure Remote Dial-Up?	Physical Security Perimeter?
B69	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.2. Substation	A	5.2.1	1						1	Part of RDRIC blackout plan.	N/A	0		N/A	N/A	N/A	N/A	N/A	N/A	N/A
B69-01	XXX	XXX	XXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		Not Applicable	0	Not Routable, Not Dial-Up		5	N/A	no	N/A	N/A	N/A
B69-02	XXX	XXX	XXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		Not Applicable	0	Not Routable, Not Dial-Up	Only for Maintenance	1	N/A	no	N/A	N/A	N/A
B69-10	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		R3.3	1		Redundant Metering at Other Stations via Dial-Up	3	3	YES	no	YES	no
B69-11	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		R3.3	1		Needed for Voltage Control and Monitoring SOL's	1	1	no	N/A	N/A	N/A
B69-12	XXX	XXX	XXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		Other	0	Serial-only, Not IP Accessible	Exempted per CIP-002-1 Applicability 4.2.2	1	N/A	no	N/A	N/A	N/A
B69-13	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		Other	1		Exempted per CIP-002-1 Applicability 4.2.2	1	1	no	N/A	N/A	N/A
B69-14	XXX	XXX	XXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	1						1		Not Applicable	0	Not Routable, Not Dial-Up	Exempted per CIP-002-1 Applicability 4.2.2	1	N/A	no	N/A	N/A	N/A
B69-15	XXX	XXX	XXXX	R1.2.2. Substation	B	5.2.1	1						1		Not Applicable	0	Not Routable, Not Dial-Up	Only Long-Term Impact	3	N/A	no	N/A	N/A	N/A
B69-16	XXX	XXX	XXXXXXXXXXXX	R1.2.2. Substation	B	5.2.1	0						1		Not Applicable	0	Will be Routable (in the future)		5	N/A	no	N/A	N/A	N/A
BCT1	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	A	5.3.2		1					1			N/A			N/A	N/A	N/A	N/A	N/A	N/A
BCT2	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	A	5.3.2		1					1			N/A			N/A	N/A	N/A	N/A	N/A	N/A
BCT3	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	A	5.3.2 & 5.4.1		1	1				1			N/A			N/A	N/A	N/A	N/A	N/A	N/A
BCT3&4-02	XXX	XXX	XXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		0	Not Routable, Not Dial-Up			5	N/A	no	N/A	N/A	N/A
BCT3&4-03	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		R3.1	1			5	5	YES	YES	no	YES
BCT3&4-04	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		R3.1	1			1	1	no	N/A	N/A	N/A
BCT3&4-05	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		0	Not Routable, Not Dial-Up			5	N/A	no	N/A	N/A	N/A
BCT3&4-06	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		0	Not Routable, Not Dial-Up			4	N/A	no	N/A	N/A	N/A
BCT3&4-07	XXX	XXX	XXXXXXXXXXXXXXXXXXXX	R1.2.3. Generation Resource	B	5.3.2 & 5.4.1		1	1				1		0	Not Routable, Not Dial-Up			4	N/A	no	N/A	N/A	N/A

# Visual Identification of Critical Assets



# Critical Assets - Risks Identified

Home • Compliance Visuals • Insight

Search All SEARCH TOOLS SETTINGS ACTIONS Projects

Search Results History

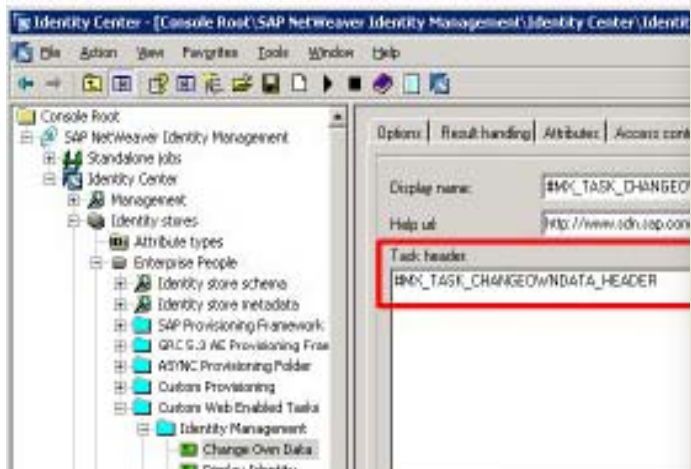
Sub-station 1 SCADA

- Network 1
- Network 2
- Network 3
- Users
- Risks
  - Terminated users have active access to the SCADA system.
  - SOA Risk-Ability to modify relays through SCADA and change access to PI Historian.
  - Critical configuration changes can be performed by a single user.
  - Terminated users have active physical access to the SCADA system.
  - Valid remote access to non-employees with admin privileges.
- Change Logs

Position Control

Welcome Joe Black

# Access approval is complex and too technical



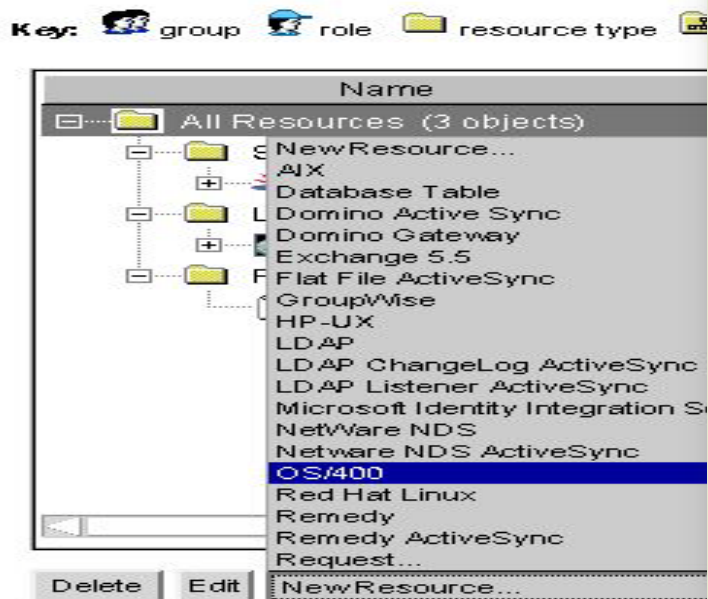
Service Name	Virsa SAP Adapter for DR1
Detail Logging	TRUE
Access Enforcer Select System URL	http://virdb2:50100/AESelectSystemService_5_2/Config1?wsdl
Tivoli Directory Integrator location	rmi://172.16.159.2:16231/ITDIDispatcher
Access Enforcer Request URL	http://virdb2:50100/AESubmitRequestService_5_2/Config1?wsdl
User Id	VIRSAITIM
System Identifier	DR1
User Id	VIRSAITIM

No workflow

avnetOrgPerson	
Full Name	Anjani Jha
Avnet Job Number	0000
Aliases	ajha1
AvnetID	ajha1
Avnet Status Code	A
First Name	Anjani
Password Last Changed Date	200705172304Z
Custom Display	ajha1
Organizational Roles	ITAM Role AD Role Enterprise LDAP role Virsa role
Last Name	Jha
Avnet Corp. Number	000
Avnet Dept. Number	0
Avnet Branch Number	0

No workflow

Manager Last Name	Smathers
Manager First Name	Bill
Requestor Email	anjani.ja@avnet.com
Manager Email	bill.smathers@avnet.com
User Last Name	Jha
Password Last Changed Date	200706042250Z
Employee Type	NEW
Request Reason	Testing Only
Requestor First Name	TBD
Company	AVNET NA
User First Name	Anjani
Requestor Last Name	VIRSAITIM
Priority	HIGH
Owner	Anjani Jha
Service	Virsa SAP Adapter for DR1
Location	PHOENIX
User Email	anjani.jha@avnet.com



# Business layer across IT and Physical Access reduces complexity

 **Request Number: 92** |  **Manager** 


**Request Category:** New Access | **User ID:** Sbailey

**First Name:** Susan | **Last Name:** Bailey

**Email:** Sbailey@harwely.com | **Telephone:** 510-310-4536



 **Comments (8)**

 **History (8)**

 **Attachments (0)**

**Details** | **Access** | **Risks (2)** | **Screening (5)**






**Show**  **Systems (5)**  **Roles (5)** **Add Role(s)** **Remove Role(s)**

	Role	Type	System	Action	From	To
<input type="checkbox"/>	Reaction Floor Area	Physical	Facility Badging System	Add	04/01/2009 	04/02/2011 
<input type="checkbox"/>	Ammonia Storage Zone	Physical	Facility Badging System	Add	04/01/2009 	04/02/2011 
<input type="checkbox"/>	Modify PLC Settings	Logical Control Systems	Plant Distributed Control	Add	04/01/2009 	04/02/2011 
<input type="checkbox"/>	Manage DCS 6	Logical Control Systems	Plant Distributed Control	Add	04/01/2009 	04/02/2011 
<input type="checkbox"/>	Manage Tier 2 substance	Logical	ERP System	Add	04/01/2009 	04/02/2011 




**Approve** **Hold** **Forward** **Reject** **Evaluate Risk** **Back**

2008 © Copyright Alert Enterprise. All rights reserved.

# Identify Systems and Applications Requiring Access

 **Request Number: 92** |  **Manager**   **Help** 







**Request Category:** New Access      **User ID:** Sbailey  
**First Name:** Susan      **Last Name:** Bailey  
**Email:** Sbailey@harwely.com      **Telephone:** 510-310-4536

 **Comments (8)**  
 **History (8)**  
 **Attachments (0)**

**Details** | **Access** | **Risks (2)** | **Screening (5)**

**Show**  **Systems (5)**  **Roles (5)**      **Add System(s)**      **Remove System(s)**

**My Systems**

	System	Owner	Action	Valid From	Valid To
<input type="checkbox"/>	Facility Badging System	Mark Truman	New User	04/01/2009 	04/02/2011 
<input type="checkbox"/>	ERP System	David Hill	New User	04/01/2009 	04/02/2009 
<input type="checkbox"/>	Plant Distributed Control Sy	Sturdy Butler	New User	04/01/2009 	04/02/2009 

**Other Systems**

**Approve** | **Hold** | **Forward** | **Reject** | **Evaluate Risk**      **Back**

2008 © Copyright Alert Enterprise. All rights reserved.

# Automated Remediation and Mitigation

The screenshot displays a web application interface for managing access requests. At the top, there is a navigation bar with 'Home', 'Reports', 'Set Up', and 'Help' buttons. A user greeting 'Welcome Joe Black' is visible in the top right. Below the navigation bar, the main content area shows details for a request with 'Request Number: 88'. The user information includes 'First Name: Ted', 'Last Name: Hawk', 'Email: ted@alert.com', and 'Telephone: 510-333-5555'. The request category is 'Change Access'. On the right side, there are links for 'Comments (0)', 'History (0)', and 'Attachments (0)'. The main content area has tabs for 'Details', 'Access', 'Risks (1)', and 'Training (1)'. A 'Show Risks' button is visible. A modal dialog box titled 'Remediate Risk' is open in the center, displaying the following text: 'The following actions will be taken to remediate the risk PHINV01 for personnel Ted Hawk.' Below this text are two checkboxes: one checked for 'Disable Ted Hawk's Physical Access to the Drug Shipment Zone.' and one unchecked for 'Disable Ted Hawk's IT Access to Inventory Control in the ERP System.' At the bottom of the dialog are 'Continue' and 'Cancel' buttons. In the background, a table lists risks, with one entry 'PHINV01: Having Drug Shipment Z...' visible. At the bottom of the page, there are buttons for 'Approve', 'Hold', 'Forward', 'Reject', 'Evaluate Risk', and 'Back'. A footer note reads '2008 © Copyright Alert Enterprise. All rights reserved.'

# Access Revoked – Risk Remediated

Home • NERC CIP D

Home • NERC CIP D

Compliance Status

Requirement

CIP002 - Critical As

CIP003 - Security M

CIP004 - Personnel

CIP005 - Electronic

CIP006 - Physical S

CIP007 - Systems S

CIP008 - Sabotage

CIP009 - Recovery

Home

Reports

Set Up

Help

Welcome Joe Black

Risk Violation Details

Risk Remediation for risk NERC CIP006-R1, CIP004-R2 for personnel Dave Jackson has been successfully performed. A request has been created to complete the process.

**Risk:** CIP006R15-002 - Terminated Personnel have valid physical access to critical cyber assets.

**Level:** High

**Compliance Requirements:** NERC CIP006-R1, CIP004-R2

**Violations:** 18

**Impact:** Personnel can gain unauthorized access to critical cyber assets leading to sabotage hurting the reliability of the Bulk Electric System (BES).

**Business Process:** Transmission Operations

**Risk Owner:** Tom McGuire

**Details:**

User	Position	System	Roles
<input type="checkbox"/> Jones Wu	Sub-station Manager	SanJose GE PP	Sub-station Control Room
<input checked="" type="checkbox"/> Dave Jackson	SCADA Operator	SanJose GE PP	Sub-station Control Room
<input type="checkbox"/> Mike Singer	Load Analyst I	SanJose GE PP	Transmission Switch Yard
<input type="checkbox"/> John Smith	Inter-connect Manager	SanJose GE PP	Sub-station Control Room
<input type="checkbox"/> Mark Doe	Load Analyst III	Corporate Honeywell	Transmission Switch Yard
<input type="checkbox"/> Lisa Ray	Generator Mechanic	Corporate Honeywell	Generator I Control Center

Remediate Risk Mitigate Risk Forward Back

Status



## Threat Scenario #2 - Smart Meter (AMI) Remote Disconnect Malicious Attempt

Scenario: John has privileged access to provision meters remotely. John was denied promotion. John attempts to remotely disconnect hundreds of meters

Insider Threat Solution should:

- Monitor criticality of access at time of provisioning
- Assign mitigating controls
- Trigger mitigating control when meters first disabled
- Generate alert and revoke access

# Visualize Plant Assets, Networks, Users and Risk

The screenshot displays the AlertEnterprise web application interface. At the top, the logo "AlertEnterprise" is followed by the tagline "True Convergence of Physical and Logical Security". Navigation tabs include "Home", "Reports", "Action", "Risk Library", "Setup", and "Help". A user greeting "Welcome Gary Higgins" is visible in the top right corner.

The main content area is titled "Home • Compliance Visuals • Insight". It features a search bar with the text "critical assets" and a "SEARCH" button. Below the search bar, a diagram visualizes the relationship between various plant assets, networks, users, and risks. The diagram shows a central "Users" node connected to several "Critical Assets" nodes: "Sub-station 1 Control Center", "Sub-station 2 Control Center", "Generation Station 1", "Generation Station 2", and "Sub-station 3 Control Center". These assets are further connected to "Network 1" and "Risks". The "Risks" node is connected to "John Doe", "MooreCh", "TayloJo", and "AnderWi". Finally, "John Doe" is connected to two risk nodes, "RK43" and "RK44".

The interface also includes a "Position Control" window in the bottom left corner and a Windows taskbar at the bottom with several open applications and a system tray showing the time as 11:58 AM.

# Ability to display risks related to Smart Meter

The screenshot shows the 'Alert Enterprise' web application interface. At the top, the browser title is 'Alert Enterprise'. Below the title bar, there are fields for user information: Request Category: NewHire, FirstName: John, UserID: JDoe, LastName: Doe, Telephone, and ValidFrom: 09/16/2009. Below this, there are tabs for 'Details', 'Access', 'Certification', 'History', 'Attachments', and 'Risks'. The 'Risks' tab is selected. Under the 'Risks' tab, there are radio buttons for 'Risks(1)' (selected) and 'Mitigation Control(0)'. A 'Mitigate Risk' button is located to the right. Below this, there is a table with the following columns: Risk, Description, Resource, Critical, Control Id, and Action. The table contains two rows of data:

	Risk	Description	Resource	Critical	Control Id	Action
<input type="checkbox"/>	<a href="#">RK43</a>	Ability to remotely disconnect meters	DA1	High		<a href="#">Add mitigation control</a>
<input type="checkbox"/>	<a href="#">RK44</a>	Unrestricted physical access to control room	DA1	High		<a href="#">Add mitigation control</a>

At the bottom of the interface, there are buttons for 'Approve', 'Hold', 'Forward', 'Reject', 'Evaluate Risks', and 'Cancel'. The Windows taskbar at the bottom shows the start button, several Microsoft Office applications, the Alert Enterprise application, a 98% battery indicator, and the system clock showing 10:39 AM on 10/16/2009.

# Threat Scenario #3 – Sabotage attempt by disgruntled employee

Scenario: Attempt to shut down grid by disabling two levels of protective relays and defeating interlocks.

A Solution must be able to:

- ➔ Identify and confirm incident
- ➔ Initiate notification workflow
- ➔ Invoke Geo-Spatial Monitoring
- ➔ Initiate Lockdown Sequence
- ➔ Notify first responders for dispatch

# Geo-spatial view of Substation

Home Reports Set Up Help Welcome Joe Black

Alert ID: 245 Severity:  Help ?

Details Events Logs Comments Attachments

**Summary:** Unauthorized disabling of 2-levels of protection relays at the Salinas Generation Facility performed. This may be a sabotage attempt.


**Impact:** Disabling of protective relays could cause a blackout and could lead to equipment damage at the sub-station.

**Personnel:** *Unknown*

**Date/Time:** 02/09/2009 19:56 PM

**Location:** Fremont Transmission Sub-Station

**Organisation:** Transmission



**Remediation Scripts**

#	Task	Priority	Status
1	Situation Analysis and Incident Confirmation	High	Closed
2	Initiate Area Lockdown and Dispatch Security Personnel	High	Open
3	Send Emergency Alerts to personnel, Law Enforcement and Management	High	Closed
4	Initiate Utility Inter-connection procedures to avoid blackout.	High	Open

**Task ID # 2** Manual

**Task:** Initiate Area Lockdown and Dispatch Security Personnel

**Assigned To:** Tom Hopkins **Priority:** High

**Start:** 25 Feb 09 10:52PM **Status:**

**Precedence:** 2 **Due By:** 25 Feb 09 10:57PM


**Comments:**


CREATE NEW TASK SAVE TASK PREVIOUS TASK NEXT TASK

Submit Reject Hold Forward Create Case Back

# High Severity – Drill Down For Detail

Home Reports Set Up Help Welcome Joe Black


Alert ID: 245 Severity:  Help ?

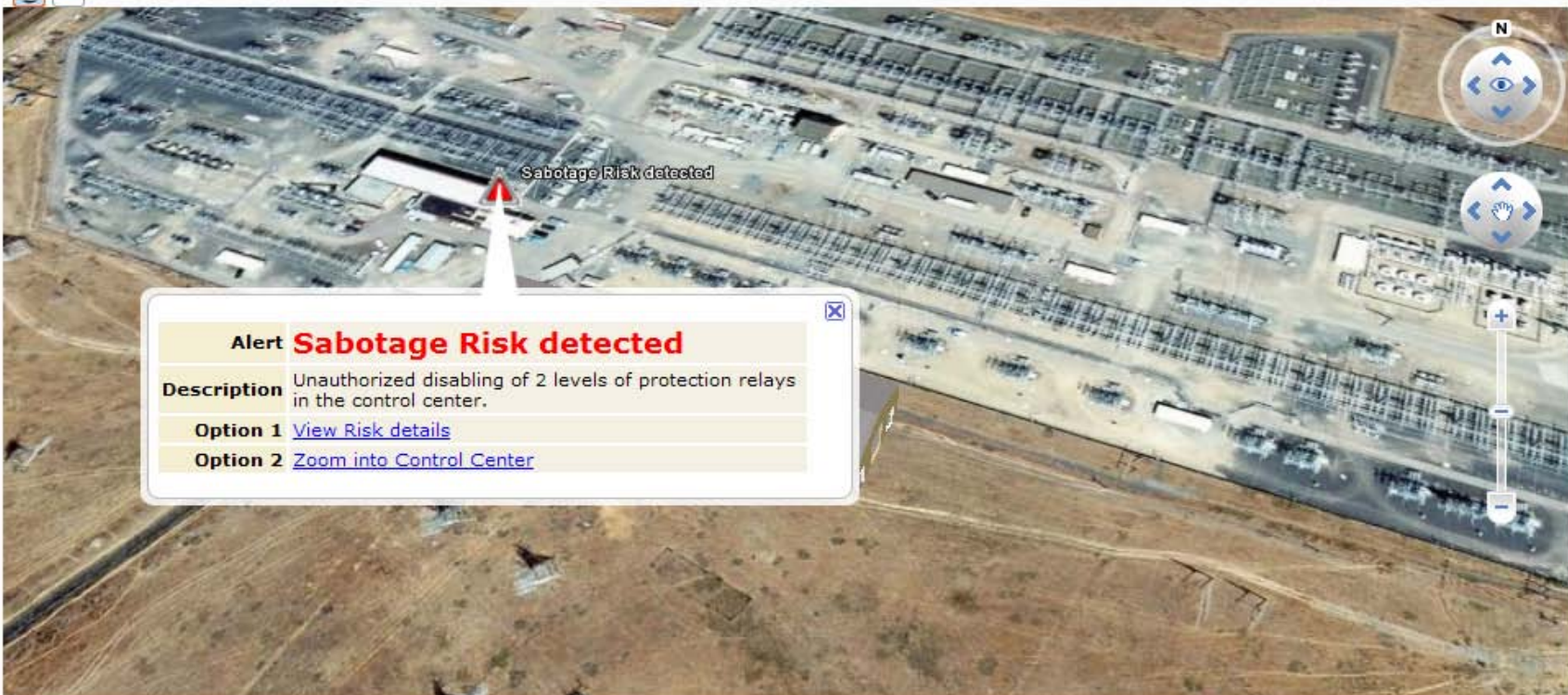


Submit Reject Hold Forward Create Case Back

# Substation - Sabotage risk!

Home Reports Set Up Help Welcome Joe Black

Alert ID: 245 Severity:  Help ?



**Alert** **Sabotage Risk detected**

**Description** Unauthorized disabling of 2 levels of protection relays in the control center.

**Option 1** [View Risk details](#)

**Option 2** [Zoom into Control Center](#)

Submit Reject Hold Forward Create Case Back

# Access Live Video & Initiate Physical Lockdown

The screenshot displays a web-based interface for "Geo-spatial Monitoring". At the top, there is a navigation bar with "Home", "Reports", "Set Up", and "Help" tabs. On the right, it says "Welcome Joe Black". Below this, an "Alert ID: 245" is shown with a "Severity" indicator (a red and yellow bar) and a "Help" button with a question mark. The main area is a 3D rendered room with rows of desks and chairs. A "Camera Options" button is positioned above a doorway, and a "Door Options" button is positioned above the doorway itself. A "Live Video Feed" window is overlaid on the left, showing a real-time camera view of the room with a timestamp of "12:56:14 PM". On the right side of the 3D view, there are navigation controls including a compass, a hand icon for panning, and a vertical zoom slider. At the bottom of the interface, there is a row of buttons: "Submit", "Reject", "Hold", "Forward", "Create Case", and "Back".



# Insider Threats Occur in the Real World.

Real World Incidents Require a World-Class Response



Management Staff



PEOPLE  
PROCESS  
TECHNOLOGY



Managers responding to incidents need real-time information on evolving threats, potential perimeter breaches and unauthorized access to critical assets.

# Best Practice Recommendations to Reduce Insider Threat

- Organizations must deal with insider threat as a security incident – not just cyber or physical or safety
- Implement systems to correlate information from ERP applications, facilities, critical assets, and control systems
- Develop an Insider Incident Response plan – leverage existing IT and Surveillance systems to deliver real-time situational awareness to operational managers
- Create a program to monitor privileged users like system administrators even closer – leverage Key Risk Indicators (KRIs) and Risk Libraries
- Terminations: Deactivate IT Access and Physical Access immediately - don't just leave it to the Guns and Guards

# AlertEnterprise Company Overview



## Flagship Customers

- Oklahoma Gas & Electric
- Allegheny Energy
- Nike
- SITA Netherland



## Most Innovative Company Awards

- RSA Conference 2009
- Security Summit 2009
- SAP TechEd Demo Jam
- ASIS Top 10 Award 2009
- GSN – Homeland Security



## Pilot Projects

- TSA – Top US Airport Security
- DHS, non-lethal weapon system



## Key Partners

- Deloitte
- PWC
- SAP
- Oracle
- Cisco



## Experienced Team with Successful Track Record

- Founded Application Security company Virsa Systems (\$400M acquisition by SAP)



## Market Advantage

- Application Security Context & Domain Knowledge

# Thank You

**Pan Kamal**

**AlertEnterprise, Inc.**

**Pan.Kamal@AlertEnterprise.com**

**AlertEnterprise!**  
True Convergence of Physical and Logical Security